Redaktion: Helmut Reimer

Report

Apps mit Datenschutzmängeln

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat im Rahmen einer internationalen Prüfungsaktion 30 Apps bayerischer Anbieter überprüft und das Ergebnis am 14.05.2013 veröffentlicht. Es wurden erhebliche Mängel bei der Information über den Umgang mit Daten festgestellt. Von der Festsetzung von Bußgeldern wird zunächst abgesehen.

Im März 2010 haben sich Datenschutz-Aufsichtsbehörden aus den Bereichen der OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung) und der APEC (Asiatisch-pazifische wirtschaftliche Zusammenarbeit) in einem Netzwerk (GPEN – Global Privacy Enforcement Network) zusammengefunden, um länderübergreifend den Datenschutz zu stärken. Für die Woche vom 5. bis 12. Mai 2013 hat dieses Netzwerk im Rahmen eines erstmals ausgerufenen „International Internet Sweep Day" die Datenschutzaufsichtsbehörden aus den 25 beteiligten Ländern aufgerufen, Webseiten im nicht-öffentlichen Bereich und mobile Applikationen (Apps) auf Transparenz im Umgang mit personenbezogenen Daten zu prüfen.

Das BayLDA hat sich an dieser Prüfungsaktion beteiligt und 30 zufällig ausgewählte Apps bayerischer Unternehmen überprüft. Im Fokus dieser Prüfung stand lediglich die Verfügbarkeit und Auffindbarkeit der Datenschutzerklärung, deren Verständlichkeit und die Erreichbarkeit der verantwortlichen Stelle, um in datenschutzrechtlichen Belangen mit dieser in Kontakt treten zu können. Welche Datenerhebungen und -übermittlungen durch Apps ausgelöst werden und ob diese den Angaben in den Datenschutzerklärungen entsprechen, wird vom BayLDA im Rahmen einer Schwerpunktprüfungstätigkeit in diesem Jahr untersucht, war aber nicht Gegenstand dieser international abgestimmten Prüfung.

„Das Ergebnis der Transparenzprüfung, dass lediglich ca. 25 % der geprüften Apps über eine appspezifische Datenschutzerklärung verfügten, ist erschreckend und deutet darauf hin, dass dem Datenschutz und damit den Grundrechten der Nutzer bei der Entwicklung von Apps offensichtlich nicht die notwendige Bedeutung beigemessen wird" so Thomas Kranig, Präsident des BayLDA zum Ergebnis der Prüfung.

Anders als in der entsprechenden Vorschrift des Telemediengesetzes (§ 13 Abs. 1 TMG), wonach die Dienstanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten informieren müssen, waren bei 75 % der geprüften Apps die Datenschutzerklärungen gar nicht oder nicht auf den konkreten Dienst abgestimmt (teilweise nur Verweis auf die Datenschutzerklärung der Webseite verfügbar). Soweit ein Abruf erst nach dem Herunterladen und dem Start der App, also möglicherweise erst nach Auslesen und Übermitteln aller Kontaktdaten auf einen Rechner irgendwo in der Welt, möglich ist, bestehen ebenfalls datenschutzrechtliche Bedenken.

Ebenso wurde in den wenigsten Fällen eine Kontaktmöglichkeit für datenschutzrechtliche Fragen und Beschwerden aufgefunden. Ein Hinweis auf die verantwortliche Stelle und ein entsprechender Kontakt konnte oftmals lediglich dem Impressum des App-Anbieters in der App oder auf der von ihm betriebenen Homepage entnommen werden.

Vielen Nutzern von Smartphones und Tablets dürfte es nicht bewusst sein, dass sie ihre „kostenlosen" Apps unter anderem mit allen ihren Kontaktdaten, d.h. den Namen, Adressen, Telefonnummern usw. von Dritten „bezahlen". Um das Bewusstsein dieser Nutzer zu sensibilisieren und zu stärken, ist es erforderlich, dass sehr transparent und sehr klar durch eine leicht aufzufindende Information erkennbar wird, ob und in welchem Umfang und zu welchen Zwecken personenbezogene Daten bei der Nutzung der entsprechenden App betroffen sind.

Das BayLDA hat erste Hinweise für die Anforderung an Datenschutzerklärungen bei Apps auf seine Homepage *www.lda.bayern.de* gestellt. Darüber hinaus wird das BayLDA bis zum Herbst nach Absprache mit den anderen Aufsichtsbehörden tiefergehende und konkrete datenschutzrechtliche Anforderungen für App-Entwickler, App-Anbieter und auch App-Nutzer auf seiner Homepage veröffentlichen.

Losgelöst von der erfolgten internationalen Prüfaktion wird das BayLDA im Herbst einen weiteren intensiveren Prüfdurchlauf vornehmen. Anbieter von Apps aus dem Freistaat Bayern, die bis dahin immer noch nicht die datenschutzrechtlichen Anforderungen erfüllen, müssen dann mit entsprechenden Bußgeldern rechnen.

Common PKI 2.0: Nachweis der Konformität vereinfacht

Ab sofort können Hersteller von Komponenten rund um die elektronische Signatur ihre zu Common PKI 2.0 konformen Produkte auf Basis einer Herstellerselbsterklärung registrieren lassen. Dies teilte der T7 e.V., die Arbeitsgemeinschaft von Trustcenterbetreibern und Zertifizierungsdiensteanbietern, am 22.05.2013 mit. Die Common PKI Spezifikation beschreibt ein Profil über international verbreitete und anerkannte Standards bei elektronischen Signaturen, Verschlüsselungen und Public Key Infrastructures (PKI). Ziel der Common PKI ist die Sicherstellung von Interoperabilität beim Einsatz von ganz unterschiedlichen konformen Produkten.

Interessierte Hersteller können jetzt ein standardisiertes Prüfprotokoll auf Basis des Common PKI Testbed vorlegen. Die Erklärung und das Protokoll werden auf der Webseite www.common-pki.org veröffentlicht. Der Common PKI Beirat des T7 e.V. möchte damit die Transparenz in Bezug auf die tatsächlich weite Verbreitung der Nutzung von Common PKI 2.0 erhöhen.

„Schon lange dient Common PKI als Basis für alle, die elektronische Signaturen anbieten, und das Testbed als i-Tüpfelchen sichert Interoperabilität von Anfang an!" sagt Dr. Rüdiger Mock-Hecker, Leiter der Geschäftssparte Kartensysteme beim Deutschen Sparkassenverlag und Vorstandsvorsitzender des T7 e.V. Auch Georgios Raptis, bei der Bundesärztekammer für HPC (Health Professional Card) und Arztausweis verantwortlich, unterstreicht die Bedeu-